Smishing, public WiFi, deepfake ... but every security threat will explode in 2020

The world of security is constantly moving, in parallel with the development speed of the internet as well as the technology field.

The world of security is constantly moving, in parallel with the development speed of the internet as well as the technology field. In addition to the introduction of more effective security methods, new threats are also becoming increasingly complex. Smishing, public WiFi, deepfake . are said to be new security threats, which are likely to explode in 2020.

As predicted by Experian computer security experts, public WiFi networks will continue to be the favorite means of spreading malicious code by hackers in 2020 due to the popularity of public internet connection systems in many cities. big in the world. Users need to be especially careful with the data they store on their phones and laptops, and carefully consider and prepare adequate safeguards before connecting to unknown public networks. .

In addition, experts also believe that "smishing" - a form of SMS phishing attack, will be popularly used by hackers in 2020. Phishing messages will mainly lurk in the form of a notice of prize winning. social, and especially politics (in some countries). This form of attack is not new, nor complicated, but still always highly effective due to the subjective, gullible gullibility of many people. Please consider before interacting with messages coming from a strange address.

Deepfake - AI-based impersonation technology (through videos, images) is often used for the purpose of creating fake news, frauds, smear, personal attacks that will be actively abused by malicious agents in 2020. For a simple example, it is possible for crooks to use deepfake technology to create fake celebrity videos to trick unsuspecting people into clicking malicious links. Or even create a fake recording in the voice of a senior management character in the company, thereby deceiving an entire organization. There are few tools capable of detecting deepfake audio and video content. Against the threat of deepfake, you will no longer be able to believe what your eyes see.

Finally, Experian warns that the growing popularity of mobile payment systems - expected to reach $ 4.5 trillion by 2023 - will be a more attractive target than ever. for scammers. While most NFC payment applications have good security systems, some devices at retail locations (such as POS) are much less secure.

Cybercriminals are constantly improving their methods of deploying their attacks in a more complex and unpredictable manner. This is why all individuals, businesses and organizations are forced to own reliable cyber security measures to protect themselves and their customers.